UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

GREG DAVIS, on behalf of himself and all others similarly situated, Plaintiff, v. COMSTAR , LLC Defendant.	Case No. 1:22-CV-11119-PBS **AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Greg Davis, through his attorneys, brings this Amended Class Action Complaint against the Defendant, Comstar, LLC ("Comstar" or "Defendant"), alleging as follows:

INTRODUCTION

1. Comstar, a Massachusetts-based ambulance billing and collections service company, lost control of patients' highly sensitive personal information in a data breach by cybercriminals ("Data Breach"). On information and belief, sometime prior to April 21, 2022, cybercriminals were able to access and pilfer Mr. Davis and Class members' information because Comstar fails to maintain adequate cyber security systems, fails to delete unneeded data with sensitive personal information, and fails to train its employees on reasonable security measures, leaving the information an unguarded target for theft and misuse. Mr. Davis used the ambulance services of one of Comstar's customers and is a Data Breach victim. He is asserting claims on behalf of himself, and all others harmed by Comstar's misconduct.

2. Comstar requires that its customers—ambulance and emergency medical service providers—disclose their patients' highly sensitive personally identifiable information and

personal health information (together "PHI") to Comstar as condition of using Comstar's billing and collection services. Comstar even prepares a form privacy notice for its customers' use. Comstar, in turn, promises to safeguard that PHI: "Your health information is personal, and Comstar is committed to protecting it."[1]

3. Comstar also promises consumers that in the event of a data breach, it will notify consumers no later than 60 days following discovery of the unauthorized use or disclosure and the date of its discovery, if known. *Id.*

4. Despite those assurances, on March 26, 2022, Comstar discovered suspicious activity related to certain of its servers. Comstar says it immediately took steps to secure its network, but it took a month for Comstar to internally confirm that third parties indeed had accessed patient information in Comstar's network, including names, dates of birth, medical assessment and medication administration, health insurance information, driver's licenses, financial account information and Social Security numbers.

5. Mr. Davis did not receive notice of the Data Breach for several months thereafter—in early July 2022.

6. Mr. Davis is not alone in this late notification; since July 2022, certain municipalities in New England that used Comstar billing services have informed the public of the Data Breach, asking residents to contact Comstar for more information.[2]

7. Despite the devastating nature of the Data Breach, on information and belief, Comstar has not offered Data Breach victims any free credit monitoring services even though the Data Breach involved Social Security numbers and dates of birth, information that Plaintiff and

[1] https://www.comstarbilling.com/privacy-policy/ (last visited July 8, 2022).
[2] https://jgpr.net/2022/07/07/town-of-hingham-shares-information-on-potential-comstar-data-breach/ (last visited July 8, 2022); https://www.golocalprov.com/news/providence-residents-who-used-city-rescue-told-their-data-possibly-breached (last visited July 8, 2022).

Class members cannot change and that cybercriminals can misuse to steal their identities.

PARTIES

8. Plaintiff, Mr. Davis, is a natural person and citizen of Rhode Island, where he intends to remain. Mr. Davis used a Providence, Rhode Island-based ambulance service in 2012 or 2014. Mr. Davis received Comstar's Breach Notice in July 2022.

9. Defendant, Comstar, is a Massachusetts limited liability company that processes medical claims, sends bills and provides collection services for ambulance service providers. Comstar's principal place of business is located at 8 Turcotte Memorial Drive, Rowley, MA 01960.

JURISDICTION & VENUE

10. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where in the amount in controversy exceeds the sum or value of $5,000,000, exclusive of costs and interest, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

11. This Court has personal jurisdiction over Comstar because Comstar is a Massachusetts entity headquartered in the Commonwealth of Massachusetts, Further, the acts or omissions giving rise to this action all took place in Massachusetts.

12. Venue is proper in this district because a substantial part of the events or omissions giving rise to the claim occurred in this District.

BACKGROUND FACTS

a. Comstar

13. Comstar is a Massachusetts-based billing and collection company providing

services to ambulance and emergency medical service providers.

14. As part of its business, Comstar collects sensitive PHI from the patients of its customers, promising to safeguard that data from theft and misuse using reasonable security measures.

15. Specifically, the PHI Comstar collects includes names, dates of birth, medical assessment and medication administration, health insurance information, driver's licenses, financial account information and Social Security numbers.

16. In so doing, Comstar recognizes its duty to safeguard PHI through its own Privacy Policy and a Notice of Privacy Practices template it maintains for its customers' use with its ambulance service users. This sample template is publicly available on Comstar's website at https://www.comstarbilling.com/online-documents/ (last visited July 8, 2022) and attached hereto as **Exhibit B**.

17. The sample Notice of Privacy Practice for "ABC Ambulance Service" tracks Comstar's Privacy Policy, stating "Your health information is personal, and [ABC Ambulance Service/Comstar] is committed to protecting it." Exh. B.

18. Despite these assurances, on information and belief, Comstar has not implemented reasonable cybersecurity safeguards or policies to protect PHI, or trained its employees to prevent, detect, and stop data breaches of Comstar's systems. As a result, Comstar leaves vulnerabilities for cybercriminals to exploit and give access to PHI.

b. Comstar Fails to Safeguard PHI

19. Plaintiff, Mr. Davis used an ambulance service in 2012 or 2014, which, upon information and belief used Comstar's services.

20. As a condition of Mr. Davis using this ambulance service, he was required to

disclose his PHI.

21. Comstar collects and maintains this PHI in its computer systems.

22. In collecting and maintaining the PHI, Comstar agreed it would safeguard the data according to its internal policies and state and federal law.

23. Still, sometime prior to April 21, 2022, cybercriminals bypassed Comstar's cybersecurity safeguards and pilfered the PHI stored in Comstar's systems.

24. Pursuant to a "Notice of Data Event" posted on its website, Comstar says that on April 21, 2022, an internal investigation of the Data Breach determined "that certain systems on our network were subject to unauthorized access." *See* **Exhibit A** (the "Breach Notice"). However, the Breach Notice says Comstar was "unable to confirm what specific information on those systems was accessed." *Id.* Following a review of the accessed systems, the Breach Notice states that "information related to certain individuals was contained therein."

25. Comstar's Breach Notice states that "the security of information in Comstar's care is one of our highest priorities and we have strict security measures in place to protect information in our care." Ex. A. However, the Breach Notice acknowledges that while it had policies and procedures in place regarding "security of information," Comstar is "reviewing those policies and procedures to further protect against similar incidents moving forward." *Id.*

26. In other words, Comstar had no effective means to quickly detect, prevent, stop, undo, or remediate the effects of the Data Breach, meaning cybercriminals could easily access and steal PHI.

27. After the breach, Comstar states it "launched a thorough investigation, with the assistance of third-party experts, to determine the nature and scope of the incident." Ex. A.

28. But Comstar disclosed little from its investigation. Indeed, the Breach Notice did

not disclose or was unable to disclose *when* cybercriminals hacked its systems, *how* Comstar allowed them to do so, *why* Comstar was unable to stop it, and *what* information hackers obtained and from whom. Instead, Comstar issued a bare-bones notice informing Data Breach victims that their highly sensitive PHI may have been compromised.

29. And despite the lifelong harm that Plaintiffs and Class members face, Comstar offered no free credit monitoring or identity theft protection to Data Breach victims.

30. On information and belief, Comstar allowed the Data Breach to occur because it failed to train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over PHI. Comstar's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PHI. Further, the Breach Notice makes clear that Comstar cannot, or will not, determine the full scope of the Data Breach, as it has been unable to determine exactly what information was stolen and when.

c. Plaintiff's Experience

31. Mr. Davis is a consumer who used ambulance services through Providence Fire Department in 2012 or 2014. Upon information and belief, this ambulance service provider is one of Comstar's customers.

32. Mr. Davis provided his PHI to the ambulance service provider, and thus also Comstar, and trusted that the Comstar would use reasonable measures to protect it according to Comstar's internal policies and state and federal law.

33. Mr. Davis has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Mr. Davis fears for his personal financial security and uncertainty over what PHI was exposed in the Data Breach. Mr. Davis has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of

the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

d. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

34. Plaintiff and members of the proposed Class have suffered injury from the unauthorized access to, theft, and misuse of their PHI that can be directly traced to Defendant.

35. As a result of Comstar's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PHI is used;

b. The diminution in value of their PHI;

c. The compromise and continuing publication of their PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PHI; and

h. The continued risk to their PHI, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the

appropriate measures to protect the PHI in their possession.

36. Stolen PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PHI can be worth up to $1,000.00 depending on the type of information obtained.

37. The value of Plaintiff and the proposed Class's PHI on the black market is considerable. Stolen PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

38. In fact, the value of this highly sensitive PHI is precisely why hackers targeted and stole it.

39. It can take victims years to spot identity or PHI theft, giving criminals plenty of time to use that information for cash.

40. One such example of criminals using PHI for profit is the development of "Fullz" packages.

41. Cyber-criminals can cross-reference multiple sources of PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

42. The development of "Fullz" packages means that stolen PHI from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz

package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

43. Defendant disclosed the PHI of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PHI of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PHI.

44. Defendant's failure to timely notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

e. Comstar Failed to Adhere to FTC Guidelines

45. According to the FTC, unauthorized PHI disclosures are extremely damaging to consumers' finances, credit history, and reputation, and can take time, money, and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

46. According to the FTC, the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best

data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PHI and PII.

47. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

48. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

49. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

50. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

51. Orders resulting from these actions further clarify the measures businesses must

take to meet their data security obligations. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ⁋ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations.

52. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PHI and PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

f. Comstar Failed to Adhere to HIPAA

53. The Health Insurance Portability and Accountability Act ("HIPAA") circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the

Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.

54. HIPAA provides specific privacy rules requiring comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is properly maintained.

55. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains, and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain, and

correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

CLASS ACTION ALLEGATIONS

56. Plaintiff brings this action on behalf of himself and the proposed Class ("Class"), pursuant to Fed. R. Civ. P. 23, defined as follows:

> All citizens whose PHI was compromised in the Data Breach disclosed by Comstar in its Breach Notice.

Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

57. Plaintiff reserves the right to amend the class definition.

a. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of approximately 69,000 members, far too many to join in a single action;

b. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

c. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. His interests do not conflict with Class members' interests and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

d. **Commonality**. Plaintiff and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PHI;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PHI;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PHI;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff and the Class injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

58. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual class members are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

59. Plaintiff realleges all previous paragraphs as if fully set forth below.

60. Plaintiff and members of the Class entrusted their PHI to Defendant. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

61. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PHI in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PHI—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PHI by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

62. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PHI. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

63. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff' and members of the Class's personal information and PHI.

64. The risk that unauthorized persons would attempt to gain access to the PHI and misuse it was foreseeable. Given that Defendant holds vast amounts of PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PHI—whether by malware or otherwise.

65. PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PHI of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

66. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PHI of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff and members of the Class's injury. Defendant further

breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

67. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

68. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customer information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive PII.

69. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its patient PHI and PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PHI and PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

70. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that,

because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

71. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PHI and PII.

72. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class members' PHI.

73. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304 definition of encryption).

74. Plaintiff and Class members are within the class of persons that the HIPAA was intended to protect.

75. The harm that occurred as a result of the Data Breach is the type of harm that HIPAA was intended to guard against. The Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures relating to protected health information, caused the same harm as that suffered by Plaintiff and the Class members.

76. Had Plaintiff and members of the Class known that Defendant did not adequately protect their PHI and PII, Plaintiff and members of the Class would not have entrusted Defendant with their PHI and PII.

77. Defendant breached its duties to Plaintiff and the Class under HIPAA, by failing

to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PHI.

78. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PHI and PII.

79. Defendant's negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PHI by criminals, improper disclosure of their PHI, lost benefit of their bargain, lost value of their PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Invasion of Privacy, Mass. Gen. Laws. Ch. 214 § 1B
(On Behalf of Plaintiff and the Class)

80. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

81. Defendant publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff and Class members by disclosing and exposing Plaintiff's and Class members' PHI to enough people that it is reasonably likely those facts will become known to the public at large, including without limitation on the dark web and elsewhere.

82. Plaintiff's and Class members' PHI, which included their names, addresses, dates of birth, Social Security numbers, driver's license numbers, account information and health information was private and intimate.

83. Defendant's disclosure of the PHI unreasonably, substantially and seriously interfered with Plaintiff's and Class members' privacy such that it offends ordinary sensibilities. Defendant should appreciate that the cyber-criminals who stole the PHI would further sell and disclose the PHI as they are doing. That the original disclosure is devastating to Plaintiff and Class members even though it may have originally only been made to one person or a limited number of cybercriminals does not render it any less a disclosure to the public-at-large.

84. The tort of public disclosure of private facts is recognized in Massachusetts under Mass. Gen Laws Ch. 214. Plaintiff's and Class members' private PHI was publicly disclosed by Defendant in the Data Breach with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendant knew and knows that Plaintiff's and Class members' PHI is not a matter of legitimate public concern.

85. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been injured and are entitled to damages.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

86. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

87. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of services through employment and through purchases of Defendant's products and services.

88. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class. Defendant also benefited from the receipt of Plaintiff and

members of the Class's PHI, as this was used to facilitate their employment and purchase of products and services.

89. Plaintiff and Class members reasonably understood that Defendant would adequately protect the PHI entrusted to it. Plaintiff and the proposed Class would not have provided their PHI, had they known Defendant would not adequately protect their PHI.

90. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Class's services, payments, and their PHI because Defendant failed to adequately protect their PHI.

91. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

COUNT IV
Violation of Massachusetts Unfair Trade Practices Act, Mass. Gen. Laws. ch. 93A
(On behalf of Plaintiff and the Class)

92. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

93. On July 12, 2022, Plaintiff sent Defendant a written demand for relief which reasonably describes the unfair and deceptive practices that Defendant committed and Plaintiff suffered, and identifies the claimant and the class they seek to represent.

94. Mass. Gen. Laws ch. 93 § 105(a) provides: "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." M.G.L. c. 93A permits any person engaged in the conduct of trade or commerce and injured by a violation of its terms to bring a civil action, including a class action, for damages and injunctive relief.

95. Plaintiff alleges that Defendant willfully and knowingly committed unfair and deceptive business acts and/or practices in violation of M.G.L. c. 93A.

96. Defendant conducts trade and commerce in Massachusetts and with Massachusetts consumers.

97. Defendant is a "person" under c. 93A § 1(a).

98. Defendant's unfair or deceptive acts or practices include: (a) failing to promptly notify the public of the Data Breach despite the existence of substantial risk to consumers from the Data Breach; and/or (b) failing to maintain reasonable safeguards sufficient to secure the private and sensitive information about Massachusetts consumers from known and foreseeable threats of unauthorized access or unauthorized use, including identity theft, financial fraud, or other harms.

99. Defendant's 93A violations actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PHI by criminals, improper disclosure of their PHI, lost benefit of their bargain, lost value of their PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about its data security practices and capabilities, the Data Breach and the stolen PHI;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 16th day of August, 2022.

By,

/s/ Michael S. Appel
Michael S. Appel, BBO #543898
SUGARMAN, ROGERS, BARSHAK & COHEN, P.C.
101 Merrimac Street, 9th Floor
Boston, MA 02114
(617) 227-3030
appel@sugarmanrogers.com

Samuel J. Strauss
sam@turkestrauss.com
Raina C. Borrelli
raina@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

Attorneys for Plaintiff and the Proposed Class

4860-1757-5982, v. 1

EXHIBIT A

Notice of Data Event

May 25, 2022 – Comstar, LLC ("Comstar") is providing notice of a recent event that may affect the security of certain information. Comstar is the billing vendor for ambulance services, and this incident did not occur at any of the ambulance providers Comstar services.

What Happened. On or about March 26, 2022, Comstar discovered suspicious activity related to certain servers within its environment. We immediately took steps to secure our network, and launched a thorough investigation, with the assistance of third-party experts, to determine the nature and scope of the incident. On April 21, 2022, the investigation determined that certain systems on our network were subject to unauthorized access. However, the investigation was unable to confirm what specific information on those systems was accessed. As such, we reviewed the contents of those systems to determine what information was contained therein and to whom it related.

What Information Was Affected. The review of the systems determined information related to certain individuals was contained within. The information varied by individual but may have included name, date of birth, medical assessment and medication administration, health insurance information, driver's license, financial account information, and Social Security number.

What We Are Doing. The security of information in Comstar's care is one of our highest priorities and we have strict security measures in place to protect information in our care. Upon becoming aware of this incident, we immediately took steps to confirm the security of our systems. While we had policies and procedures in place at the time of incident regarding security of information, we are reviewing those policies and procedures to further protect against similar incidents moving forward. We are notifying potentially impacted individuals, including you, so that you may take steps to help protect your information, should you feel it is appropriate to do so. Comstar notified law enforcement and is cooperating with the investigation. We are also reporting to state and federal regulatory officials, as required.

What Affected Individuals Can Do. Individuals are encouraged to remain vigilant against incidents of identity theft by reviewing account statements and credit reports for unusual activity and reporting any suspicious activity immediately to their financial institution. Additional detail can be found below in the *Steps You Can Take to Help Protect Your Information.*

For More Information. Individuals who have questions about this incident or believe they may be impacted by this incident, can contact our dedicated call center at 877-587-4280, Monday through Friday, except holidays.

Steps You Can Take To Help Protect Your Information

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim.

Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

*For California residents***:** Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Kentucky residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

For District of Columbia residents: the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents: the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Comstar is located at 8 Turcotte Memorial Drive, Rowley, MA 01969.

For New Mexico residents: you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents: the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents: the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

For Rhode Island residents: the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.

For Washington D.C. residents: the Office of Attorney General for the District of Columbia can be reached at: 441 4thStreet NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; https://oag.dc.gov.

For All U.S. residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338).

EXHIBIT B

NOTICE OF PRIVACY PRACTICES

ABC Ambulance Service

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IF CAREFULLY

Your health information is person, and ABC Ambulance Service is committed to protecting it. We are required by law to maintain the privacy of health information that could be used to identify you (PHI). The law requires us to provide you with a copy of this Notice of Privacy Practices (Notice), which describes our privacy practices and our legal duties with respect to PHI. Under certain circumstances, we may also be required to notify you following a breach of unsecured PHI.

HOW WE MAY USE OR DISCLOSE YOUR PHI

Treatment. We may use or disclose your PHI in connection with our treatment or transportation of you. For example, we may disclose your PHI to doctors, nurses, technicians, medical students or any other health care professional involved in taking care of you. We may also provide information about you to a hospital or dispatch center via radio, telephone or other electronic means. We may provide a hospital or other health care facility with a copy of the medical records created by us in the course of treating or transporting you.

Payment. We may use and disclose your medical information to obtain payment from you, an insurance company or other third parties. For example, we may provide PHI to your health insurance plan in order to receive payment for our services.

Health care operations. We may use and disclose your PHI for quality assurance activities, licensing and training programs to ensure that our personnel meet our standards for care, and to ensure that our personnel follow our established policies and procedures. We may also use your information for obtaining legal, financial or accounting services, conducting business planning, processing complaints, and for the creation of reports that do not individually identify you.

Other uses or disclosures that do not require authorization. The law permits us to use or disclose your PHI without your authorization in the following circumstances:

- When required by law, but only to the extent required by law.
- For public health activities, including disclosures to public health authorities authorized by law to collect information for the purpose of preventing or controlling disease, injury or disability, for reporting births and deaths, and for the conduct of public health investigations. We may also be required by law to disclose information related to possible child abuse or neglect.
- To a social service or other protective services agency authorized by law to receive reports about victims of abuse, neglect or domestic violence. We will make every effort to obtain your permission before releasing this information; however, in some cases, we may be required or authorized by law to act without your permission.
- For health oversight activities.
- For judicial and administrative proceedings, in response to a court order, subpoena, discovery request or other lawful process.
- For law enforcement purposes, including disclosures: (i) to comply with laws requiring the reporting of certain types of injuries, (ii) made pursuant to a court order, warrant, subpoena, grand jury subpoena or other lawful process, (iii) to assist law enforcement in identifying or locating a suspect, fugitive, material witness or missing person, (iv) about the victim of a crime, if, under the circumstances, we are unable to obtain your permission, (v) about a death we reasonably believe may be the result of a crime, (vi) about a crime committed on our premises, or (vii) to notify law enforcement of the commission of a crime, the location of a victim or to identify the perpetrator of a crime, but only in emergency situations.
- To coroners, medical examiners and funeral directors.
- To organ procurement organizations.
- For approved medical research projects.
- To avert a serious threat to health or safety.
- For military and veterans activities, national security and other specialized government functions
- To comply with laws relating to workers' compensation or similar programs.

USES OR DISCLOSURES WHERE YOU HAVE THE RIGHT TO OBJECT

Unless you object, we may provide relevant portions of your PHI to a family member, friend or other person that you indicate is involved in making decisions about your health care, or in paying for your health care. We may use or disclose PHI to notify your family member, friends or personal representative about your condition. In an emergency or when you are not capable of agreeing or objecting to these disclosures, we will disclose your PHI only to the extent we reasonably believe such disclosure to be in your best interest, and we will tell you about such disclosure after the emergency has passed, and give you the opportunity to object to future disclosures to family, friends or personal representatives. Unless you object, we may also disclosure your PHI to persons involved in providing disaster relief, for example, the American Red Cross.

USES OR DISCLOSURES THAT REQUIRE YOUR WRITTEN CONSENT

Any other use or disclosure of PHI, other than those listed above will only be made with your written authorization. The law also requires your written authorization before we may use or disclose: (i) psychotherapy notes, other than for the purpose of carrying out our treatment, payment or health care operations purposes, (ii) any PHI for our marketing purposes or (iii) any PHI as part of a sale of PHI. You may revoke a previous written authorization in writing at any time. If you elect to revoke a previously authorization, we will immediately stop any further uses or disclosures of your PHI for the purposes set out in the written authorizations to the extent we have not already acted in reliance on your authorization; however, we will be unable to retract any disclosures previously made with your permission.

FUNDRAISING [Note: this is optional, and should be included only if you intend to use PHI for fundraising purposes**]**

ABC Ambulance Service may use your PHI for certain fundraising activities. For example, we may use your name, your home or work address, phone number or other information in order to contact you to raise money to support our operations. We may also share this information with a charitable foundation that may contact you to raise money on our behalf. You have the right to elect to opt out of such fundraising communications. If you do not want to be contacted for our fundraising efforts, you can submit a written request to our Privacy Officer. You can also opt out of fundraising communications by calling the following toll free number: **[**800-555-5555**]**. Each time we contact you with respect to fundraising, we will remind you of this right to opt-out of future fundraising communications. In no event with the provision of medical care be conditioned on your willingness to receive fundraising communications.

YOUR RIGHTS WITH RESPECT TO YOUR PHI

You have the following rights with respect to your PHI:

- The right to request restrictions on the use and disclosure of your PHI. To exercise this right, you must submit a written request to our Privacy Officer. We are not required to agree to your request; however, if we do agree, we will put our agreement in writing, and will abide by that agreement exception to the extent the use or disclosure of such PHI is necessary to provide you treatment in an emergency. Notwithstanding the foregoing, we must agree to a restriction on the use or disclosure of your PHI if: (i) the disclosure is for our payment or health care operations purposes and is not otherwise required by law and (ii) you or another person acting on your behalf has paid for our services in full.
- The right to request to receive your PHI in a specific location (for example, at your work address rather than your home) or in a specific manner (for example, by email rather than regular mail). We will comply with all reasonable requests. Any such request should be made in writing to our Privacy Officer.
- The right to inspect and copy your PHI, except in limited circumstances. Any such request should be made in writing to our Privacy Officer. We will respond to your request within 30 days. The law gives us the right to deny your request in certain instances; in which case, we will notify you in writing of the reasons for the denial and explain your rights with regard to having the denial reviewed. A reasonable fee may be charged for making copies.
- The right to request that we amend your PHI to the extent you believe it is inaccurate or incomplete. Any such request should be made in writing to our Privacy Officer, and should include the reasons you believe that your information is inaccurate or incomplete. We will respond to your request within 60 days. We are not required to change your information, but if we do not agree to change your information, we will notify you of the reasons for our decision, and will explain your rights to submit a written statement of disagreement, to file a complaint, or to request that your requested change be included in any future disclosures of your PHI. If we agree to a change, we will ask you who else you would like us to notify of the change.
- The right to receive an accounting of any disclosures of your PHI made within the 6 years immediately preceding your request. We are not required to provide you an accounting of disclosures: (i) made for our treatment, payment or health care operations purposes, (ii) made to directly to you, your family or friends, (iii) made for national security purposes, to law enforcement or certain other governmental purposes. We are also not required to provide an accounting of disclosures made prior to April 14, 2003. If you request more than one accounting within a 12 month period, we may charge you a reasonable fee for each additional accounting.
- The right to receive a paper copy of this Notice.

NOTIFICATION IN THE EVENT OF AN UNAUTHORIZED USE OR DISCLOSURE

[Optional Provision]

The law may require us to notify you in the event of an unauthorized use or disclosure of your unsecured PHI. To the extent we are required to notify you, we must do so no later than 60 days following our discovery of such unauthorized use or disclosure. This notification will be made by first class mail or email (if you have indicated a preference to be notified by email), and must contain the following information:

- A description of the unauthorized use or disclosure, including the date of the unauthorized use or disclosure and the date of its discovery, if known.
- A description of the type of unsecured PHI that was used or disclosed.
- A description of the steps you should take to protect yourself from potential harm resulting from the unauthorized use or disclosure.
- A brief description of what we are doing to investigate the breach, to protect against future breaches, and to mitigate the harm to you.
- A way to contact us to ask questions or obtain additional information.

CHANGES TO THIS NOTICE

ABC Ambulance Service is required to comply with the terms of this Notice as currently in effect. We reserve the right to change or amend our privacy practices at any time in the future, and to make any changes applicable to PHI already in our possession. This Notice will be revised to reflect any changes in our privacy practices. You may obtain a copy of our revised Notice by contacting our Privacy Officer. We will also make any revised Notice available on our website at: **[**http://www.abcambulance.com.**]**

CONTACT

If you would have questions or comments about our privacy practices, or if you would like to obtain additional information regarding your privacy rights, please contact our Privacy Officer at: **[**ABC Ambulance Service, 123 Main Street, Anywhere USA 99999**]**. You may also contact our Privacy Officer by phone at: 800-555-5555.

COMPLAINTS

If you believe that your privacy rights have been violated, you may file a complaint with ABC Ambulance Service or with Secretary of the Department of Health and Human Services (DHHS). To file a complaint with us, please put your complaint in writing and mail it to the following address: **[**Privacy Officer, ABC Ambulance Service, 123 Main Street, Anywhere USA 99999**]**. You may also contact our Privacy Officer by phone at: **[**800-555-5555**]**. To file a complaint with the DHHS, you must put your complaint in writing and mail it to: Office for Civil Rights, U.S. Department of Health and Human Services, 200 Independence Avenue, S.W., Washington, D.C. 20201. You will not be retaliated against or denied any health services if you elect to file a complaint.

[Note: you may substitute the corresponding OCR Regional Office for the OCR Headquarters. The addresses for the 10 Regional Offices can be found at: http://www.hhs.gov/ocr/office/about/rgn-hqaddresses.html**]**

Effective Date: April 14, 2003

Revision Date: March 26, 2013